

# User authentication using gait and enhanced attribute-based encryption: a case of smart home

Lim Wei Pin, Manmeet Mahinderjit Singh

School of Computer Sciences, University Sains Malaysia, Penang, Malaysia

## Article Info

### Article history:

Received Nov 27, 2022

Revised Oct 19, 2023

Accepted Dec 7, 2023

### Keywords:

Biometrics

Cryptographic

Passwordless

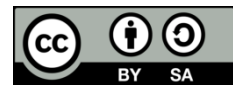
Machine learning

Encryption

## ABSTRACT

With the increasing popularity of the internet of things (IoT) application such as smart home, more data is being collected, and subsequently, concerns about preserving the privacy and confidentiality of these data are growing. When intruders attack and get control of smart home devices, privacy is compromised. Attribute-based encryption (ABE) is a new technique proposed to solve the data privacy issue in smart homes. However, ABE involves high computational cost, and the length of its ciphertext/private key increases linearly with the number of attributes, thus limiting the usage of ABE. This study proposes an enhanced ABE that utilises gait profile. By combining lesser number of attributes and generating a profiling attribute that utilises gait, the proposed technique solves two issues: computational cost and one-to-one encryption. Based on experiment conducted, computational time has been reduced by 55.27% with nine static attributes and one profile attribute. Thus, enhanced ABE is better in terms of computational time.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



## Corresponding Author:

Manmeet Mahinderjit Singh

School of Computer Sciences, University Sains Malaysia

11800 Penang Malaysia

Email: manmeet@usm.my

## 1. INTRODUCTION

Smart homes are filled with connected products aiming to make life smarter and easier. However, several challenges confront smart homes in the IoT context, including interoperability issues, where different devices and systems must work together for optimised performance [1]. Real-time data processing should be considered, and existing frameworks are not sustainable [2]. The issues of security and privacy are another challenge given the large number of devices that are susceptible to attack. The data collected are sensitive personally identifiable information. Thus, these data must be handled carefully to prevent any disclosure of information. One preventive measurement besides the usage of encryption in securing data would be employ authentication mechanism. Simple authentication methods that require only username and password combinations are inherently vulnerable to brute force, phishing, key logging and even man in the middle leading to personal data being stolen for unethical purpose. One countermeasure technique is by adopting passwordless authentication method.

Smart homes face serious data security and privacy issues. Various attacks can lead to data privacy issues, such as time, location, data, and user-based privacy attacks. Many smart home devices have sensors that constantly capture user activities. The information transmitted from smart homes to the cloud can be captured by network observers to infer privacy-sensitive activities. Three categories of solutions aim to solve the data privacy issue in smart homes: policy based [3], cryptography based [4], and data anonymisation based [5]. Policy-based solutions create a set of rules or policies to determine data access, such as using the

Jess language to create a policy to ensure data privacy in the cloud [6]. Cryptography-based solutions use encryptions, such as attribute-based encryption (ABE), to encrypt the data before transmitting them to the cloud. Compared with the two other kinds of solutions, cryptography-based solutions using ABE require no architectural redesign and can be implemented in either a legacy or a new system. However, ABE has limitations, such as computational time and the linear increase in the length of the ciphertext scale with the number of attributes. Therefore, ABE is not suitable for one-to-one-encryption owing to its lack of unique attributes. Gait, on the other hand, can provide the user with a unique identity. In this research, ABE with gait profiling will be explored. The usage of gait or human movement such as walking, standing etc is taken into context. Gait, being a biometric is a suitable candidate for designing passwordless based authentication model. A gait profile will be built and combined with ABE to provide one-to-one encryption and reduce the number of attributes used. This enhanced ABE can improve data privacy in smart homes by providing a unique identity for one-to-one encryption.

The objectives of this research are to; i) design and evaluate an enhanced clustering and classification algorithm to generate a gait profile, ii) propose an enhanced gait profile for user identification, and iii) build an enhanced ABE technique using the generated gait profile. This research focuses on a cryptography-based solution that uses ABE. Moreover, it attempts to create a behavioural profile using gait, which is unique to a user, to substitute for the multiple attributes needed to identify a person. The outline of the paper is as follows. Section 2 present the related work. Section 3 present proposed work and section 4 discuss the experimental results. Finally, section 5 depicts the conclusion and future work.

## 2. STATE OF ART

With almost 30 billion connected devices globally in 2025, more than 500 billion Gbs of data at rest and in transit will be generated from these devices' sensors and processing tasks. According to [7], [8], the vast amount of data generated and processed will result in several challenges to the IoT field, including data integration, real-time processing, and security and privacy. Vulnerability exists within smart device applications, such as smart homes due to characteristics of the devices and its operating modes. The features of sensors within a connected application are always 'on', attentive to contextual settings, and interconnected as well as operate anytime and anywhere. Next, description on smart home is presented.

### 2.1. An example of internet of thing-smart home security

A smart home refers to a house where all the electronic devices are connected and capable of communicating with one another. Smart home devices range from temperature sensors, humidity sensors, and smart lights to smart speakers, smart TVs, and smart air conditioners [9]. However, connecting smart home appliances to the internet makes the users vulnerable to malicious attacks. Private information gathered by sensor data—such as health data, shopping preferences, and eating habits—can be stolen by intruders [10]. This risk is particularly true for data gathered in smart homes because these data are sensitive personally identifiable information [11].

A smart hub in a home is designed to control sensors and devices. It also receives information from all the devices connected to it, and if something happens or goes wrong, it immediately notifies its user via phone, SMS, or email in accordance with the user's preferences. At that moment, all settings are packed in the *config.jar* file, which the hub then downloads and implements.

What happens when someone can interrupt the smart home's system and gain control over the home controllers? Figure 1 shows an example of a smart device, a smart bulb that is connected to a Wi-Fi network and controlled over a mobile application.

Based on Figure 1, one of the security threats on the hub is due to the open access of the hub's firmware, which could be publicly downloaded. Once the firmware is accessed, other files within the firmware could be easily analysed as well. Another threat is the lack of strong cryptographic services protecting the firmware files. The password from the root account in the shadow file is encrypted with the data encryption standard algorithm. As practice shows, this cryptographic algorithm is not secure or highly resistant to hacking. Therefore, an attacker can successfully obtain the hash through brute force and find the 'root' password. Another vulnerability in *config.jar* beyond login credentials is the IP addresses and device IDs for all the devices connected in the home. The manipulation of settings, such as modifying sensitive details, becomes possible. The *config.jar* file also consists of the owner's phone number, which is meant to receive alerts and notifications. Another vulnerability point is the smart devices connected within the smart home. To set the smart bulb, a user needs to download the mobile application (iOS or Android), switch on the bulb, connect to the Wi-Fi access point created by the bulb, and then provide the bulb with the SSID and password from a local Wi-Fi network. A hacker can easily launch a man-in-the-middle attack on the device and manipulate the settings as long as the hacker shares the same local Wi-Fi network as the smart home system.

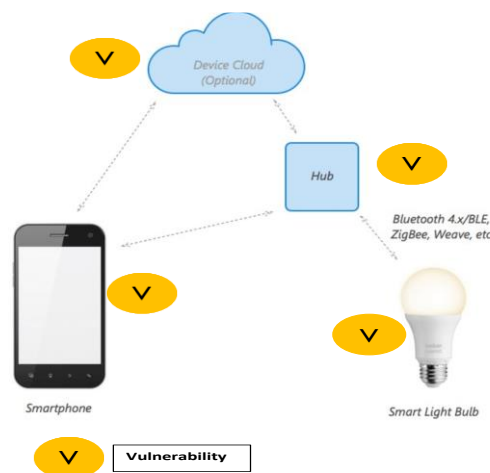


Figure 1. Smart home security vulnerabilities

## 2.2. Attribute-based encryption concept

The concept of ABE was first introduced by [12], who presented a scheme called fuzzy identity-based encryption (FIBE), which is the fundamental of ABE. ABE is a type of public key cryptosystem where the secret key of a user and the ciphertext created are based on a set of attributes. ABE has significant advantages; it is a flexible one-to-many encryption method and is a promising tool for securing fine-grained data sharing and decentralised access control. Almost all existing ABE schemes admit that reasonably expressive decryption policies produce ciphertext whose size depends at least linearly on the number of attributes involved in the policy [13]. However, three challenges are associated with ABE: performance, key revocation, and collusion resistance. In term of performance, data overhead increases with the number of attributes because the attributes are translated into an access tree that grows as a function of attributes embedded in the encryption key and ciphertext. A full performance evaluation of ABE shows that data overhead occurs in ABE [14]. The issue of performance owing to a large number of attributes not only affects the accuracy of ABE but also fails to provide sound security protection. In addition, this variant of ABE may not be able to be employed for the IoT environment which is lightweight based [15]. Based on the original ABE, some variants of ABE for the IoT environment have been proposed. Table 1 lists some of the ABEs suitable for IoT and the benefits they provide.

Table 1. Attribute-based encryption for IoT applications

	Threshold policy	Key policy	Ciphertext policy	Pre-computation	Efficient revocation	Scalability
FIBE [12]	✓					
KP-ABE [12], [16]		✓				
CP-ABE [17]			✓		✓	
HABE [18]			✓			✓
MA-ABE [19]	✓	✓				✓
C-CP-ABE [20]			✓			
ECC-ABE [21]		✓	✓	✓		

Different ABE variants have been devised to solve expressive structure, scalability, and efficiency issues. In targeting ABE in an IoT environment, the schemes focus on either the pre-computation method or algorithm efficiency. However, none focus on attribute selection in ABE. Most schemes require an authority to distribute the attributes.

## 2.3. Attributes and user and entity behavioural analytics

User and entity behavioural analytics are a type of machine-learning model that uses advanced analysis and aggregate data from logs or other types of information to figure out a certain activity or behaviour. Some user behavioural profiling methods include mouse dynamics, keystroke dynamics, and gait dynamics. The three types of gait recognition are machine vision based, floor sensor based, and wearable sensor based [21]. Machine vision-based technology captures gait using video cameras, while floor sensor-based technology extracts gait through installed sensors on the floor. Wearable sensor-based technology collects gait data using bodywear motion detectors, such as accelerometers and gyroscopes. The

challenge of gait dynamics is that it is easily affected by different factors, such as sickness or other physical changes in one's body caused by injury. A better way would be to combine gait dynamics with other biometric systems. Gait is classified as a human biometric that represents human daily activities [22]. This study will focus on the use of both clustering and classification algorithms to create a profile that is unrestricted to a predefined model for user identification.

### 3. PROPOSED METHOD

The two most important aspects in this study are the proposed user profiling framework and the integration of the user profile in ABE. In the proposed framework of user profiling, a dataset goes through data pre-processing, which includes feature selection. All features go through the ensemble feature selection algorithms.

#### 3.1. Proposed framework of user profiling

The proposed framework can be divided into two parts: the training phase and the verification phase. In the training phase, data are collected first. Users perform activities such as walking, sitting, and lying down. Accelerometer and gyroscope data are collected through smartphones or wearables. The three-axial raw data are then transferred to the data pre-processing steps, where each datum undergoes filtering to filter out noise. Feature extraction is done because raw data cannot give any meaningful information. Each raw datum is sampled in a fixed window size, and feature extraction is carried out by calculating various time and frequency domain variables. Next, after all the features are extracted, feature selection begins. Only features that are closely related to the model are selected. Feature selection is used to reduce the dimensionality of the data. The ensemble feature selection technique [23] is used in feature selection. After selection, the features go through clustering algorithms for activity recognition.

#### 3.2. Proposed method using K-mean algorithm and DBScan algorithm

The next step after feature selection is activity recognition. In a real-world scenario, when users perform various activities, the system cannot know what activities the users are performing precisely. Thus, a clustering algorithm is used to cluster each of these activities. Here, the K-mean algorithm is used to cluster the data. This algorithm has several significant disadvantages. First, the number of clusters  $K$  must be specified. Second, the algorithm can only detect hyperspherical clusters that are well separated. Third, it is sensitive to noise and outlier points because these points can affect the centroid being used in the cluster. Fourth, it is highly sensitive to the selection of initial centres. Improper initialisation might cause empty clusters, slow convergence, and bad local minima. A new K-mean initialisation algorithm will be proposed in this research. The proposed initialisation algorithm is a density-based clustering algorithm that groups point near one another. The advantage of the DBSCAN algorithm is that it is robust to outliers.

In standard CP-ABE, the trusted authority learns all the attributes of a person. However, the computational time increases with the number of attributes. These attributes are also static attributes that can be contained by two persons. To solve this problem, human gait profiling is utilised. Figure 2 demonstrates on proposed enhanced attribute-based encryption. Instead of only static attributes, the users first train their gaits, and then the trusted authority can get the gait profile of the user.

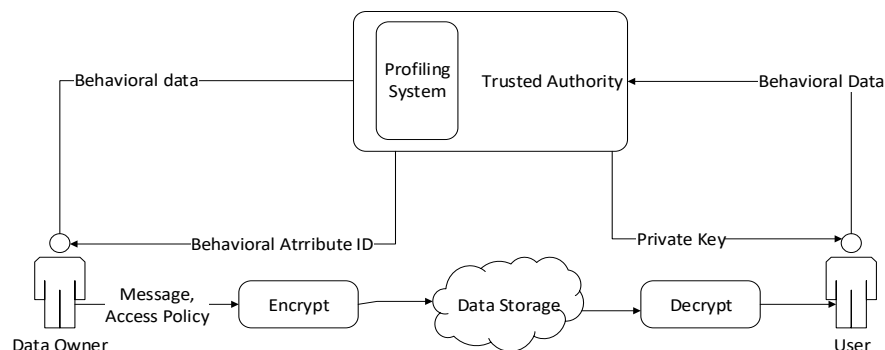


Figure 2. Proposed enhanced attribute-based encryption

Users can include this attribute profile during encryption. During decryption, users present their gait data to a trusted authority, who then compares the gait data with the profile stored in the database.

#### 4. RESULTS AND DISCUSSIONS

The discussion is divided into two parts: the user profile result and the ABE result. As mentioned earlier, the dataset used in this research is ‘Human Activity Recognition Using Smartphones’ from the UCI machine-learning repository [24]. The dataset contains all 561 features that have been extracted. To prevent a curse of dimensionality, the ensemble feature selection technique is applied. With the use of the five feature selection techniques, 16 features are selected based on the consensus list.

##### 4.1. Clustering algorithm result in gait profile creation

After 16 features are selected, they go through clustering algorithms for activity recognition. The experiments are completed according to different clustering algorithms: K-mean, canopy, EM, and farthest first. Five iterations are done on different seeds. Table 2 shows that it is crucial to choose the correct seed number to attain higher accuracy.

Table 2. Accuracy of four clustering algorithms

Seed	Farthest first (%)	EM (%)	Canopy (%)	K-mean (%)
10	47.7	84.4	76.3	98.1
100	80.3	84.4	55.6	67.5
1,000	81.04	84.4	79.7	98.1
10,000	42.3913	84.4	91.1	98.1
Highest %	81.04	84.4	91.1	98.1

All the experiments are executed using WEKA tool [25], with the ‘classification via clustering’ meta-classifier having the same training and test set. From the result, the K-mean algorithm can provide the highest accuracy, followed by the canopy, EM, and farthest-first algorithms. The EM algorithm gives the most stable result, which is 84.4%, even with different numbers of seeds. Farthest first, canopy, and K-mean are sensitive to seed number because different numbers affect their accuracy. The K-mean algorithm provides the highest accuracy but is also sensitive to the seed number chosen.

##### 4.2. Classification algorithm result in gait profile pattern matching

The results of the classification models are shown in Tables 3 and 4. Three algorithms are tested: support vector machines (SVM), random forest, and K-nearest neighbour (K-NN). The confusion matrix of the walking model is shown in Table 4. In Tables 3 and 4, A is accuracy; TPR is true positive rate; FPR is false positive rate; P is precision; R is recall; F is F-measure; ROC is receiver operating characteristics curve; PRC is precision-recall curve; and K is kappa statistic. The best result is highlighted.

Table 3. Walking model using different algorithms

Algorithms	A	TPR	FPR	P	R	F	MCC	ROC	PRC	K	Time
K-NN	80.7	0.81	0.01	0.81	0.81	0.81	0.80	0.90	0.58	0.80	<b>0.1</b>
Random forest	<b>87.9</b>	<b>0.88</b>	<b>0.004</b>	<b>0.88</b>	<b>0.88</b>	<b>0.88</b>	<b>0.88</b>	<b>1.00</b>	<b>0.93</b>	<b>0.87</b>	4.98
SVM	50.6	0.51	0.02	0.52	0.51	0.50	0.49	0.95	0.42	0.49	1.61

Table 4. Sit\_stand model using different algorithms

Algorithms	A	TPR	FPR	P	R	F	MCC	ROC	PRC	K	Time
K-NN	51.8	0.518	0.017	0.521	0.518	0.519	0.502	0.752	0.3	0.5009	<b>0.1</b>
Random forest	<b>71.1</b>	<b>0.711</b>	<b>0.01</b>	<b>0.715</b>	<b>0.711</b>	<b>0.71</b>	<b>0.702</b>	<b>0.967</b>	<b>0.754</b>	<b>0.7007</b>	4.44
SVM	8.9	0.09	0.039	0.099	0.09	0.064	0.05	0.675	0.073	0.0509	1.09

Three activity models are tested. Laying on the bed activity result is not being shared. Based on the results shown in Tables 3 and 4 and laying on bed activity result, random forest outperforms the other two classifiers by providing the highest accuracy across all three activities (i.e., 87.9% in walking, 71.1% in sit\_stand, and 87% in laying. Among the three algorithms, K-NN requires the least time to build the model, whereas random forest takes the longest time. A trade-off between accuracy and performance can be seen from the different models created.

##### 4.3. Result of enhanced attribute-based encryption

The trusted authority in ABE needs a user profile to build a profiling system. The performance of the enhanced ABE in time and length of the ciphertext is discussed in this section. Table 5 shows the computational time of ABE according to different stages in the algorithm.

Table 5. Computational time of ABE

Number of attributes	Setup(s)	Keygen(s)	Encrypt(s)	Decrypt(s)
10	0.0199	0.0533	0.0824	0.0113
30	0.0197	0.154	0.188	0.0162
50	0.0197	0.2564	0.2918	0.02144
70	0.02019	0.3604	0.4014	0.0275
90	0.0199	0.4611	0.5037	0.0332

The computational time is shown to increase with the number of attributes in all stages except for the setup. The setup stage requires a similar time to compute regardless of the number of attributes. In the decryption stage, the time to decrypt is also higher when the number of attributes increases, but it is negligible compared with those of the keygen and encryption stages. Typically, in an ABE application, around five to ten static attributes are used. However, the use of static attributes cannot identify a unique person. More attributes are needed to increase the accuracy of identifying a unique person. However, this will cause the computational time of ABE to increase significantly, which the enhanced ABE can solve. Using nine static attributes and one profile attribute can reduce the computational time to about 55.27%. Thus, enhanced ABE is better in terms of computational time. To test the security of the enhanced ABE, different case studies in which one case study will be discussed next. The case studies have three users: Alice, Bob, and Trudy.

#### Case study 1.

**Alice's Attributes** Student, CS, Security  
**Bob's Attributes** Lecturer, CS, Security  
**Trudy's Attributes** Student, CS, Security  
**Policy** CS and Security and Lecturer

#### Situation:

Alice encrypts the file with policy and wants Bob to decrypt it. Bob decrypts the file. Trudy tries to decrypt the file, although she is not authorised to do that.

#### Result:

```
Client Alice created - has attribute Student, CS, Security,
Client Bob created - has attribute Lecturer, CS, Security,
Client Trudy created - has attribute Student, CS, Security,
Alice encrypt with policy - CS AND Security AND Lecturer OR Alice
Alice decrypt with it profile attribute...Success Decrypt!
Bob decrypt but do not have it profile attribute...Success Decrypt!
Truder pretend to be Alice to decrypt but do not have it profile attribute...SK does not satisfies the policy!
Cannot Decrypt!
```

In case study 1, Alice and Bob can decrypt the ciphertext, not Trudy. This is true because Bob contains attributes that satisfy the policy and is expected to be able to decrypt the file. Alice is able to decrypt the ciphertext, although her attributes do not satisfy the policy because the policy is created using Alice's profile attribute. Trudy has the same attributes as Alice but is not able to decrypt the file because she does not have Alice's profile attribute. Next section focuses on discussion.

## 4.4. Discussions

A comprehensive discussion is presented based on several scenarios:

### a. Clustering and classification algorithms

Existing gait profile creation focuses on classification algorithms [26], [27]. However, using only classification algorithms requires a predefined model trained earlier. The proposed method uses clustering algorithms to cluster different gaits into different groups, and then these groups of data will be saved as user gait models. During verification, the unknown data will first be clustered into different groups, and the classification algorithm will be used to find the match of the user gait model created earlier. Thus, user identification is achieved. The advantage of this method is that users are not restricted to a predefined gait model, and thus, it can be used to create a more practical application.

### b. Proposed enhanced attribute-based encryption

ABE is a one-to-many encryption algorithm, and thus, achieving one-to-one encryption is impossible in normal ABE. This problem can be solved with the proposed enhanced ABE. Data owners can choose to use one-to-many encryption or one-to-one encryption. In normal ABE, if the policy that the data owner specifies does not match the data owner's attributes, then they will not be able to decrypt the data. With the enhanced ABE, the use of profile attributes allows the data owner to decrypt their own data.

### c. Comparison with normal attribute-based encryption

Normal ABE is a one-to-many encryption system, which means one party can encrypt the data, while multiple parties can decrypt it. This is different from normal public key encryption, which is a one-to-one encryption system. In one-to-one encryption, a key exchange is needed by both parties to enable the decryption process. The advantage of one-to-one encryption is that it allows only the desired party to decrypt the data. The only possible way is to create more attributes to describe the person. However, using more

attributes increases the computational cost. By utilising gait as one of the attributes in ABE, the enhanced ABE allows both one-to-one and one-to-many encryption.

## 5. CONCLUSION

The proposed framework has several limitations that can be considered in future work. First is pertaining to the gait biometric adopted. Gait is chosen to build the profile. The disadvantage of gait is that posture variation will affect accuracy. This is the current problem of using gait as a profile. Sickness or injuries will affect the gait model of the user. Additional research must be conducted to solve this issue. Next, limitation revolves the method chosen which is K-Means. The initialisation method employs the idea of the density-based cluster algorithm DBSCAN to achieve its purpose. Overall, the proposed enhanced ABE will hopefully be more suitable for use in the IoT world.

## ACKNOWLEDGEMENT

This work is supported by the Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme with project code FRGS/1/2020/ICT07/USM/02/2.




## REFERENCES

- [1] J. Ko, A. Terzis, S. Dawson-Haggerty, D. E. Culler, J. W. Hui, and P. Levis, "Connecting low-power and lossy networks to the internet," in *IEEE Communications Magazine*, vol. 49, no. 4, pp. 96-101, April 2011, doi: 10.1109/MCOM.2011.5741163.
- [2] B. L. R. Stojkoska and K. V. Trivodaliev, "A review of Internet of things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, part 3, pp. 1454-1464, 2017, doi: 10.1016/j.jclepro.2016.10.006.
- [3] S. Moncrieff, S. Venkatesh, and G. West, "Dynamic Privacy in a Smart House Environment," *2007 IEEE International Conference on Multimedia and Expo*, Beijing, China, 2007, pp. 2034-2037, doi: 10.1109/ICME.2007.4285080.
- [4] R. Chowdhury, H. Ould-Slimane, C. Talhi, and M. Cherié, "Attribute-Based Encryption for Preserving Smart Home Data Privacy," *International Conference on Smart Homes and Health Telematics ICOST 2017: Enhanced Quality of Life and Smart Living*, Paris, France, Springer, 2017, pp. 185-197, doi: 10.1007/978-3-319-66188-9\_16.
- [5] F. Z. Berrehili and A. Belmekki, "Privacy Preservation in the Internet of Things," in *Advances in Ubiquitous Networking 2: Proceedings of the UNet'16*, Springer, 2017, pp. 163-175.
- [6] S. A. Bagüés, A. Zeidler, C. F. Valdivielso, and I. R. Matias, "Sentry@Home — Leveraging the smart home for privacy in pervasive computing," *International Journal of Smart Home*, vol. 1, no. 2, pp. 129-145, 2007.
- [7] A. Banafa, IoT Implementation and Challenges, 2016, Available online: <https://www.bbvaopenmind.com/en/technology/digital-world/iot-implementation-and-challenges/>.
- [8] M. Daniele, S. Sicari, and F. De Pellegrini, "Internet of Things: Vision, Applications, and Research Challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497-1516, doi: 10.1016/j.adhoc.2012.02.016.
- [9] S. Makonin, L. Bartram and F. Popowich, "A Smarter Smart Home: Case Studies of Ambient Intelligence," in *IEEE Pervasive Computing*, vol. 12, no. 1, pp. 58-66, 2013, doi: 10.1109/MPRV.2012.58.
- [10] D. Pishva and K. Takeda, "A Product Based Security Model for Smart Home Appliances," *Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology*, Lexington, KY, USA, 2006, pp. 234-242, doi: 10.1109/CCST.2006.313456.
- [11] Federal Trade Commission. Internet of things: Privacy & security in a connected world. Washington, DC: Federal Trade Commission. 2013, Available online: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> (accessed: 23 August 2020).
- [12] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," *Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2005: Advances in Cryptology – EUROCRYPT 2005*, Springer, Berlin, Heidelberg, 2005, vol. 3494, pp. 457-473, doi: 10.1007/11426639\_27.
- [13] C. Wang and J. Luo, "An efficient key-policy attribute-based encryption scheme with constant ciphertext length," *Mathematical Problems in Engineering*, vol. 2013, 2013, pp. 1-7, doi: 10.1155/2013/810969.
- [14] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT," *2014 IEEE International Conference on Communications (ICC)*, Sydney, NSW, Australia, 2014, pp. 725-730, doi: 10.1109/ICC.2014.6883405.
- [15] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of things," *Future Generation Computer Systems*, vol. 49, 2015, pp. 104-112, doi: 10.1016/j.future.2014.10.010.
- [16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *CCS '06: Proceedings of the 13th ACM conference on Computer and communications security*, 2006, pp. 89-98, doi: 10.1145/1180405.1180418.
- [17] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," *2007 IEEE Symposium on Security and Privacy (SP '07)*, Berkeley, CA, USA, 2007, pp. 321-334, doi: 10.1109/SP.2007.11.
- [18] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," *CCS '10: Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 735-737, doi: 10.1145/1866307.1866414.
- [19] M. Chase, "Multi-authority attribute based encryption," *Theory of Cryptography Conference TCC 2007: Theory of Cryptography*, Springer, Berlin, Heidelberg, 2007, vol. 4392, pp. 515-534, doi: 10.1007/978-3-540-70936-7\_28.
- [20] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative Ciphertext Policy Attribute-Based Encryption for the Internet of Things," *2014 International Conference on Advanced Networking Distributed Systems and Applications*, Bejaia, Algeria, 2014, pp. 64-69, doi: 10.1109/INDS.2014.19.
- [21] D. Gafurov, "A Survey of Biometric Gait Recognition: Approaches, Security, and Challenges," in *Annual Norwegian Computer Science Conference*, 2007.




- [22] W. Yang, Y. Wang, and G. Mori, "Recognizing human actions from still images with latent poses," *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, San Francisco, CA, USA, 2010, pp. 2030-2037, doi: 10.1109/CVPR.2010.5539879.
- [23] Ç. B. Erdaş, I. Atasoy, K. Açıcı, and H. Oğul, "Integrating features for accelerometer-based activity recognition," *Procedia Computer Science*, vol. 98, pp. 522–527, 2016 doi: 10.1016/j.procs.2016.09.070
- [24] D. Anguita, A. Ghio, L. Oneto, X. Parra and J. L. Reyes-Ortiz, "A Public Domain Dataset for Human Activity Recognition Using Smartphones," *Sensor*, vol. 20, no. 8, pp. 1-14, 2010, doi: 10.3390/s20082200
- [25] M.Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The WEKA Data Mining Software: An Update," *SIGKDD Explorations*, vol. 11, no. 1, 2009.
- [26] R. Damaševičius, R. Maskeliūnas, A. Venčkauskas, and M. Woźniak, "Smartphone user identity verification using gait characteristics," *Symmetry*, vol. 8, no. 10, pp. 1-20, 2016, doi: 10.3390/sym8100100.
- [27] H. M. Thang, V. Q. Viet, N. Dinh Thuc and D. Choi, "Gait identification using accelerometer on mobile phone," *2012 International Conference on Control, Automation and Information Sciences (ICCAIS)*, Saigon, Vietnam, 2012, pp. 344-348, doi: 10.1109/ICCAIS.2012.6466615.

## BIOGRAPHIES OF AUTHORS



**Lim Wei Pin**    is a Master Student in School of Computer Sciences. His research focus on cryptographic based applications and protocols. He can be contacted at email: limwp.student@usm.my.



**Dr. Manmeet Mahinderjit Singh**    is an Associate Professor at the School of Computer Science. She was awarded a PhD Degree in Data Security from the School of Electrical Engineering, from University of Queensland, Australia, in 2012, and an M.Sc. in Computer Science from University of Sains Malaysia. Her research interests are primarily in information security, smart security, and sensor network security where she is the author/co-author of over 70 research publications. She can be contacted at email: manmeet@usm.my.